

IN THE CLAIMS:

Please amend the claims, as follows:

Claim 1 (Currently amended): A server that provides service to a client ~~services to clients connected to the server via a network, the server comprising:~~

~~a public-key storage unit for storing a public key assigned to each service provided by the server;~~

~~a challenge generator for generating a challenge to be sent from the server to the client after the server receives a request for [[a]] the service from the client; and~~

~~an access privilege verifier for verifying, using a corresponding public key, whether a prescribed relationship exists between the challenge transmitted to the client and a response to that challenge received from the client; and~~

~~wherein the response is calculated based on a unique operation for the client and access privilege proving that data is created from a private key corresponding to the public key.~~

~~a controlling unit, while authenticating access privilege of the client for a service provided by the server,~~

~~for transmitting the challenge generated by the challenge generator to the client;~~

~~for receiving the response to that challenge returned from the client;~~

~~for verifying, with an access privilege verifier using a public key assigned to the service and stored in the public-key storage unit, whether a prescribed relationship exists between the challenge and the response; and~~

~~for providing the service to the client only when the access privilege verifier~~

~~successfully verifies the relationship.~~

Claims 2-8 (Canceled).

Claim 9 (Currently amended): A server as recited in claim 1, wherein the server is a web server that supplies a web applications application to clients the client; and the public keys key stored in the public-key storage unit are is assigned to an individual web pages page provided to the clients and are used to verify the access privileges of the client for a web page when the server receives a request from the client to access a web page.

Claim 10 (Canceled).

Claim 11 (Currently amended): A server as recited in claim 1, wherein the server is a web server that supplies a web applications application to clients; and the public keys key stored in the public-key storage unit are is assigned to groups of web pages provided to the clients and are is to verify the access privileges of the client for a the web page when the server receives a request from the client to access a web page in one of the groups of web pages.

Claim 12 (Canceled).

Claim 13 (Currently amended): A server ~~that provides services to clients connected to the server via a network, the server comprising:~~ as recited in claim 1, further comprising:

a script interpreter for interpreting script designed to control the contents of services service, that the server provides to clients and for controlling the operations of the server, and

a privilege authenticator for authenticating access privileges of the client when called by the script interpreter.

Claims 14 - 15 (Canceled).

Claim 16 (Currently amended): A method executed in a server for providing service to a client services from the server to clients connected to the server via a network after verifying the access privileges of the clients for the services, public keys being whererin a public key is assigned in advance to a service respective services provided by the server, the method comprising the steps of:

generating a challenge when a request for [[a]] the service is received from [[a]] the client and transmitting the challenge to the client;

transmitting the challenge to the client; receiving a response to the challenge returned from the client;

verifying whether that a prescribed relationship exists between the challenge sent to the client and the response received from the client by using the public key assigned to the requested service; and

providing the requested service to the client only when the prescribed relationship exists.; wherein the response is calculated based on a unique operation for the client and a private key corresponding to the public key.

Claim 17 (Currently amended): A method executed in a client for proving its access privilege for a server when requesting a service from ~~to~~ a server connected to the client via a network, the client being in advance assigned with a unique operation, the requested service being in advance assigned with a public key, the client in advance receiving access privilege proving data for expressing the access privilege of the client for the service, the access privilege proving data being created from a private key corresponding to a public key assigned to the service and the result of a unique operation assigned to the client, the method comprising the steps of:

receiving a challenge from the server;

executing ~~the a~~ unique operation assigned to the client wherein the unique operation is unique to the client thereto;

generating a response based on the challenge received from the server, the result of the unique operation, ~~and the access privilege proving data~~; and

transmitting the response to the server.

Claims 18 - 21 (Canceled).

Claim 22 (New): A system comprising:

a server that provides service to a client;

the server further comprising:

a public-key storage unit that stores a public key assigned to the service;

a challenge generator that generates a challenge to be sent from the server to the client after the server receives a request for the service from the client;

an access privilege verifier that verifies whether a prescribed relationship exists between the challenge and a response, the response being corresponding to the challenge and received from the client, and

the client that requests the service to the server;

the client further comprising:

an unique operation executer that executes an unique operation assigned to the client;

a response generator that generates the response to the challenge, the challenge being received from the server,

wherein the response is calculated based on the unique operation and a private key corresponding to the public key, and the unique operation is unique to the client.

Claim 23 (New): The system according to claim 22, wherein the server sends the challenge to the client with a condition for using the service.

Claim 24 (New): The system according to claim 22, wherein the unique operation is used under conditions that a common cryptographic hash function is assigned to all clients and different data is assigned to each client.

Claim 25 (New): A client that requests service to a server, comprising:

an unique operation executer that executes a unique operation assigned to the client;

an access privilege providing data storage unit that stores access privilege

providing data, the access privilege providing data being created from a private key corresponding to a public key assigned to the requested service and a result of the unique operation;

a response generator that generates a response to a challenge, the challenge being received from the server, and

wherein the response is calculated based on the result of the unique operation and the access privilege providing data, and the unique operation is unique to the client.

Claim 26 (New): The client according to claim 25, wherein the access privilege providing data storage unit is included in a portable device.